

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 2 of 19

Attorney's Docket No.: 10664-147001

Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A computer-implemented method for transmitting a message from a sender to an intended recipient comprising:
 - encrypting a message using a symmetric key to generate an encrypted message;
 - sending the encrypted message to an intended recipient without making the symmetric key immediately accessible to the intended recipient;
 - providing the symmetric key to a third party; and
 - if the intended recipient signs and returns to the third party a receipt including a representation of the encrypted ~~for the message~~, transferring, by the third party, the receipt to a sender and providing the symmetric key to the intended recipient.
2. (Previously Presented) The computer-implemented method of claim 1 wherein the receipt signed by the recipient contains an identifier computed from the message and the symmetric key using cryptographically secure hash functions.
3. (Currently Amended) A computer-implemented method for transmitting a message from a sender to an intended recipient comprising:
 - at a sender, encrypting a message using a symmetric key, encrypting the symmetric key to make the symmetric key accessible to a third party but not immediately accessible to an intended recipient and sending the encrypted message and the encrypted symmetric key to the intended recipient;
 - at the recipient, signing a receipt including a representation of ~~for the~~ encrypted message and sending the receipt and the encrypted symmetric key to the third party; and

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 3 of 19

Attorney's Docket No.: 10664-147001

at the third party, transferring the receipt to the sender and providing the symmetric key to the intended recipient if the receipt is properly signed.

4. (Previously Presented) A computer-implemented method for certifying receipt of a message, the message being sent from a sender to an intended recipient and being encrypted by a symmetric key, and the method executing at a third party distinct from the sender and the recipient, the method comprising:

- receiving a signed receipt and an encrypted symmetric key from an intended recipient, the signed receipt memorializing receipt of the encrypted message by the intended recipient;
- verifying the signed receipt;
- transferring the verified receipt to a sender; and
- providing the symmetric key to the intended recipient.

5. (Previously Presented) A computer-implemented method for certifying receipt of a message, the message being sent from a sender to an intended recipient and being encrypted by a symmetric key, the method executing at a third party distinct from the sender and the recipient, the method comprising:

- receiving a separately encrypted message header associated with the message and a certified receipt originating from an intended recipient, the certified receipt including a message identifier signed by the intended recipient;

- decrypting the separately encrypted message header to expose a symmetric key and the message identifier;

- verifying the certified receipt including verifying the signature of the intended recipient and the message identifier in the certified receipt is the same as the message identifier obtained from the separately encrypted message header;

- forwarding the certified receipt to the sender; and

- forwarding the symmetric key to the intended recipient.

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 4 of 19

Attorney's Docket No.: 10664-147001

6. (Previously Presented) A computer-implemented method for transmitting a message from a sender to an intended recipient comprising:

- encrypting a message using a symmetric key;
- storing the symmetric key and the message;
- sending the encrypted message to an intended recipient without the symmetric key;
- forwarding the encrypted symmetric key to a third party; and
- receiving from the third party a certified receipt verified by the third party indicating receipt of the message by the intended recipient.

7. (Previously Presented) A computer-implemented method for transmitting a message from a sender to an intended recipient comprising:

- identifying a message for transmission to an intended recipient;
- creating a message header that includes a symmetric key and a message identifier associated with the message;
- encrypting the message using the symmetric key;
- public key encrypting the message header using a public key of a third party;
- attaching the message header to the encrypted message forming a certified message and forwarding the certified message to the intended recipient;
- storing a copy of the certified message and the symmetric key;
- receiving a certified receipt originating from an intended recipient, the certified receipt being verified at the third party and forwarded to the sender after verification; and
- verifying validity of the receipt using the stored symmetric key and the certified message.

8. (Previously Presented) A computer-implemented method for providing a receipt for a message, the message being sent from a sender to an intended recipient and the method executing at the recipient, the method comprising:

- receiving an encrypted message from a sender, the message encrypted by a symmetric key;

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 5 of 19

Attorney's Docket No.: 10664-147001

creating a receipt for the encrypted message including signing a hash of the encrypted message and returning the signed receipt to a third party;

after verification of the signed receipt at the third party, receiving the symmetric key from the third party; and

decrypting the encrypted message using the symmetric key.

9. (Previously Presented) The computer-implemented method of claim 8 wherein the step of receiving the symmetric key includes not receiving the symmetric key until a successful transfer of the signed receipt to the sender.

10. (Previously Presented) The method of claim 6, further comprising:
verifying the validity of the certified receipt using the stored symmetric key and the certified message.

11. (Currently Amended) A computer-implemented method for ~~computing a message identifier~~ generating a receipt associated with a message, where the receipt is created without exposing the content of the message to an intended recipient ~~a third party~~, comprising:

receiving a message encrypted by a symmetric key;

receiving a hash of the symmetric key; and

generating a receipt including ~~generating a message identifier~~ prior to decrypting the message, the message identifier including a representation of the hash of the symmetric key and the message encrypted by the symmetric key; and

sending the message identifier along with an associated message to an intended recipient of the message, wherein the message identifier able to be viewed by a third party is able to be used to verify receipt of the message at the intended recipient without exposing the message content to an intended recipient ~~to the third party~~.

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 6 of 19

Attorney's Docket No.: 10664-147001

12. (Currently Amended) The computer-implemented method of claim 11, wherein:
generating a receipt including a message identifier ~~the representation of the hash of the~~
~~symmetric key and the message encrypted by the symmetric key~~ includes using a hash function.
13. (Currently Amended) The computer-implemented method of claim 11, further comprising:
receiving the a first message identifier at the intended recipient;
the generating step including generating a receipt including the a second message
identifier, at the intended recipient; and
sending the receipt and the first message identifier to ~~the~~ a third party.
14. (Currently Amended) The computer-implemented method of claim 13, further comprising:
receiving the receipt, at the third party;
verifying the receipt without accessing the message content; and
providing the receipt to a sender.
15. (Currently Amended) The computer-implemented method of claim 11, ~~further~~
~~comprising where:~~
the message is encrypted encrypting the message with the symmetric key prior to sending
to the recipient; and
sending the symmetric key is sent to the intended recipient from ~~the~~ a third party so that
the intended recipient can decrypt the message.
16. (Currently Amended) The computer-implemented method of claim 11, further comprising:
sending the encrypted symmetric key to the intended recipient with the message;

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 7 of 19

Attorney's Docket No.: 10664-147001

at the intended recipient, sending the encrypted symmetric key to ~~the~~ a third party with
~~thea receipt that includes a representation of the message identifier;~~ and
sending the receipt to a sender after verification of the receipt.

17. (Currently Amended) A computer-implemented method for generating a signed receipt associated with a message without exposing the content of the message ~~to a third party,~~ comprising:

receiving a message encrypted by a symmetric key;
receiving a hash of the symmetric key;
generating a representation of the hash of the symmetric key and the message encrypted
by the symmetric key; and
signing the representation to generate a signed receipt;
wherein the receipt is generated prior to decrypting the message and receiving the
symmetric key; and
~~— sending the signed receipt to a third party for transfer to a sender.~~

18. (Currently Amended) The computer-implemented method of claim 17, further comprising:

sending the signed receipt to a third party for transfer to a sender; and
verifying the validity of the signed receipt at the third party.

19. (Previously Presented) The computer-implemented method of claim 18, further comprising:

allowing a recipient access to the content of the message if the signed receipt is verified
at the third party.

20. (Previously Presented) A computer-implemented method for time-stamping a message without exposing the content of the message to a time stamping authority, comprising:

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 8 of 19

Attorney's Docket No.: 10664-147001

encrypting the message using a symmetric key;
computing a hash of the symmetric key;
generating a representation of the hash of the symmetric key and the message encrypted
by the symmetric key; and
time-stamping the representation.

21. (Previously Presented) The computer-implemented method of claim 20, wherein:
time-stamping the representation includes sending the representation to a time-stamping
authority and receiving from the time-stamping authority a time stamp certificate including the
representation and a time.

22. (Currently Amended) The A computer-implemented method of claim 20, wherein for
time-stamping a message without exposing the content of the message to a time stamping
authority, comprising:
encrypting the message using a symmetric key;
computing a hash of the symmetric key;
generating a representation of the hash of the symmetric key and the message encrypted
by the symmetric key; and
time-stamping the representation, ~~including~~includes sending the representation to a time-
stamping authority and receiving from the time-stamping authority a time stamp certificate
including the representation, a time, a sender identification and a recipient identification for the
message.

23. (Currently Amended) The A computer-implemented method of claim 20, wherein for
time-stamping a message without exposing the content of the message to a time stamping
authority, comprising:
encrypting the message using a symmetric key;
computing a hash of the symmetric key;

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 9 of 19

Attorney's Docket No.: 10664-147001

generating a representation of the hash of the symmetric key and the message encrypted by the symmetric key; and:

time-stamping the representation, ~~includes including~~ sending the representation to a time-stamping authority and receiving from the time-stamping authority a time stamp certificate including the representation, a time, a sender identification and a recipient identification for the message and at least one of a public key of the sender and a public key of the recipient.

24. (Currently Amended) A computer-implemented method for generating a signed receipt certifying that a message has been received at a particular time by an intended recipient, without exposing the message content to a third party, comprising:

receiving a message having content, wherein the message is encrypted by a symmetric key;

receiving a hash of the symmetric key;

generating a representation of the hash of the symmetric key and the message encrypted by the symmetric key, wherein the representation is generated prior to decrypting the message and receiving the symmetric key;

time-stamping the representation; and

signing the time-stamped representation;

and

~~_____ sending the time-stamped representation to a third party such that the time stamp can be verified by the third party without exposing the content of the message to the third party.~~

25. (Currently Amended) The computer-implemented method of claim 24, further comprising:

sending the time-stamped representation to a third party such that the time stamp can be verified by the third party without exposing the content of the message to the third party; and
verifying the validity of the signed receipt at the third party.

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 10 of 19

Attorney's Docket No.: 10664-147001

26. (Previously Presented) The computer-implemented method of claim 25, further comprising:

allowing an intended recipient access to content of the message if the signed receipt is verified at the third party.

27. (Currently Amended) A computer-implemented method for generating a signed receipt for a message certifying a sending time and a receiving time by an intended recipient without exposing the content of the message to a third party, comprising:

receiving a message encrypted with a symmetric key;
receiving a hash of the symmetric key;
receiving a time-stamped representation of the hash of the symmetric key and the encrypted message, the representation being time-stamped at time of sending;
time-stamping the representation at a time of receiving;
combining the representation time-stamped at the time of sending and the representation time-stamped at the time of receiving providing a combined receipt; and
signing the combined receipt; and
sending the combined receipt to a third party such that the combined receipt can be verified by the third party without exposing the content of the message to the third party.

28. (Previously Presented) The computer-implemented method of claim 27, further comprising:

verifying the validity of the signed receipt at the third party.

29. (Previously Presented) The computer-implemented method of claim 27, further comprising:

allowing an intended recipient access to content of the message if the signed receipt is verified at the third party.

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 11 of 19

Attorney's Docket No.: 10664-147001

30. (New) The computer-implemented method of claim 1, further comprising:
computing a hash of the symmetric key; and
making the hash of the symmetric key accessible to the intended recipient, wherein the receipt contains a representation of the symmetric key.
31. (New) A computer-implemented method for securing sending a message, comprising:
encrypting a message using a symmetric key;
computing a hash of the symmetric key; and
generating a representation of the hash of the symmetric key and the message encrypted by the symmetric key.
32. (New) The computer-implemented method of claim 31, wherein:
generating the representation includes using a one-way hash.
33. (New) The computer-implemented method of claim 31, further comprising:
sending a request including the representation to a time stamping authority;
receiving from the time stamping authority a time stamp certificate including a time stamped representation of the hash of the symmetric key and the message encrypted by the symmetric key;
constructing a certified message including the time stamp certificate; and
sending the certified message to a recipient.
34. (New) A computer-implemented method for computing a message identifier associated with a message comprising:
encrypting a message using a symmetric key to generate an encrypted message;
computing a hash of the symmetric key; and
generating a representation of the hash of the symmetric key and the encrypted message.

Attorney's Docket No.: 10664-147001

Applicant : Gary Liu
Serial No. : 09/826,320
Filed : April 3, 2001
Page : 12 of 19

35. (New) The computer implemented method of claim 34 wherein generating the representation of the hash of the symmetric key and the encrypted message including using a one-way hash function.

36. (New) A computer-implemented method of for securely sending and receiving a message, using a third party to verify the authenticity of the message, comprising:

at a sender:

- encrypting a message using a symmetric key to generate an encrypted message;
- sending the encrypted message to an intended recipient without making the symmetric key immediately accessible to the intended recipient; and
- providing the symmetric key to a third party;

at the intended recipient:

- receiving the encrypted message from the sender;
- creating a signed receipt for the encrypted message, including signing a hash of the encrypted message and returning the signed receipt to the third party;
- after verification of the signed receipt at the third party, receiving the symmetric key from the third party; and

- decrypting the encrypted message using the symmetric key;

at the third party:

- receiving the signed receipt from the recipient;
- verifying the signed receipt;
- transferring the verified receipt to the sender, and
- providing the symmetric key to the intended recipient.